REMARKS

The Applicant and the undersigned thank Examiner Nalven for his careful review of this application.

Claims 1-57 have been rejected by the Examiner. Upon entry of this amendment and Request for Continued Examination (RCE), Claims 2, 5, 15, 41, and 51 remain cancelled while Claims 1, 3-4, 6-14, 16-40, 42-50, and 52-57 remain pending in this application. The six independent claims are Claims 1, 14, 25, 37, 50, and 56.

Consideration of the present application is respectfully requested in light of the above claim amendments to the application and in view of the following remarks.

Claim Rejections Under 35 U.S.C. §§ 103

The Examiner rejected Claims 1, 3-4, 6, 14, 18-21, 25-26, 32, 34-35, 37-40, 42, 50, 52 and 54-56 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Pat. No. 6,301,668 issued in the name of Gleichauf et al. (hereinafter, "the Gleichauf reference") in view of a printed publication, entitled "Firewalls" authored by Steinke (hereinafter, the "Steinke-Firewalls publication"), and further in view of U.S. Pat. No. 6,460,141 issued in the name of Olden et al. (hereinafter, the "Olden reference"). The Examiner rejected Claims 7-8, 10-12, 22, 29-31, 43-44, 46-48, and 57 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf, Steinke-Firewalls publication, and Olden references and further in view of U.S. Pat. No. 5,991,881 issued in the name of Conklin et al. (hereinafter, the "Conklin reference").

The Examiner rejected Claims 9, 23, and 45 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference, the Steinke-Firewalls publication, the Olden reference, the Conklin reference, and further in view of U.S. Patent Application Publication No. 2002/0083331, published in the name of Krumel (hereinafter, the "Krumel reference"). The Examiner rejected Claims 13 and 49 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference, the Steinke-Firewalls publication, the Olden reference, the Conklin reference, and further in view of a Printed Publication entitled, "Detecting Backdoors," authored by Zhang et al. (hereinafter, the "Zhang publication").

The Examiner rejected Claims 17 and 53 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference, the Steinke-Firewalls publication, the Olden reference, and further

in view of a Printed Publication entitled, "Security Reality Check," authored by Farrow (hereinafter, the "Farrow publication").

The Examiner rejected Claim 24 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference, the Steinke-Firewalls publication, the Olden reference, the Conklin reference, the Krumel reference, and further in view of the Zhang publication. The Examiner rejected Claim 28 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference, the Steinke-Firewalls publication, the Conklin reference, and further in view of the U.S. Patent No. 6,275,942 issued in the name of Bernhard et al (hereinafter, the "Bernhard reference"). The Examiner rejected Claims 33 and 36 under 35 U.S.C. § 103(a) as being unpatentable over the Gleichauf reference in view of the Steinke-Firewalls publication, Olden, and Krumel references.

The Applicant respectfully offers remarks to traverse these pending rejections. The Applicant will address each independent claim separately as the Applicant believes that each independent claim is separately patentable over the prior art of record.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang, Farrow publication, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a plurality of data signatures relevant to computer security; (2) designating an alert condition value to each data signature based on (3) each data signature itself and (4) contextual information associated with the data signature, (5) each alert condition value comprising a ranked value that (6) is unique to each combination of data signature and contextual information associated with a particular data signature, (7) the contextual information comprising at least one of (8a) an application layer data field type used to encapsulate the data signature and (8b) an application layer protocol type used to transmit the data signature, (9) the alert condition value indicating a security risk level (10) relative to different data signatures and (11) relative to other identical data signatures associated with different contextual information; (12) creating a table comprising contextual information, the data signatures, and the alert condition values; (13) detecting a data signature by evaluating communications at an application layer level between a target and a suspect; (14) correlating said data signature with an application layer fingerprint of the target to determine to what extent said target is vulnerable to said data

signature; (15) evaluating contextual information related to the data signature by comparing the contextual information and the data signature to the table (16) in order to determine a likelihood that said target is under attack; and (17) assigning an alert condition value to the data signature based on (18) the comparison of the contextual information and data signature to data in the table, as recited in amended independent Claim 1.

Support for Contextual Information Table

The Applicant respectfully submits that the additional elements of the contextual information table described in the amended independent claims are fully supported by the original disclosure. Specifically, the contextual information table recited in the independent claims is illustrated in original Figure 4 reproduced below. The description of Figure 4 is found in paragraph [0044] of the original application text on page 16.

Contextual Information for Data Signature Evaluation

Data Signature	Context	Severity/Alert Condition (0-5)
"/cgi-bin/phf"	HTTP URL	4
"/cgi-bin/phf"	Email header	0
"/cgi-bin/phf"	HTML HREF	3
".exe"	TFTP filename	2

FIG. 4

The Gleichauf Reference

The Gleichauf reference generally describes a system 20 for adaptive network security using network vulnerability assessment. The network environment can comprise devices that form an internal network, protection for the internal network, and an external network. The

internal network, indicated generally at 10, can comprise a plurality of workstations 12 coupled to a network backbone 14. Network backbone 14 can comprise, for example, an Ethernet, FDDI, token ring, or other type of network backbone. Protection for internal network 10 can be provided by firewall 16 and a router 18 which are coupled to network backbone 14. Router 18 serves as a gateway between internal network 10 and an external network 30. External network 30 can be, for example, the Internet or other public network. Firewall 16 can serve to limit external access to resources in internal network 10 and protect these internal resources from unauthorized use. See Figure 2 of the Gleichauf reference reproduced below, and in column 4, lines 40-58.

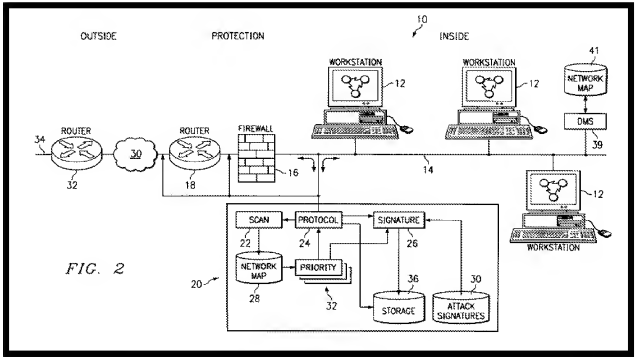


FIG. 2

Internal network 10 of the Gleichauf reference further comprises a network security system 20 coupled to network backbone 14. The network security system 20 can include a scan engine 22 and a protocol engine 24 coupled to network backbone 14. A signature engine 26 is coupled to protocol engine 24. The scan engine 22 is further coupled to network map 28. The signature engine 26 is coupled to attack signatures 30. A priority engine 32 is coupled to network map 28, protocol engine 24 and signature engine 26. The protocol engine 24 and signature engine 26 are each also coupled to a storage 36. See the Gleichauf reference, column 4, lines 58-68.

The Gleichauf reference explains that the protocol engine 24 performs a plurality of protocol analyses upon monitored traffic on network backbone 14 in order to detect attacks upon the network. Attacks upon the network include unauthorized accesses, policy violations, and patterns of misuse. The protocol engine 24 can perform the following protocol analyses upon monitored traffic on network backbone 14: checksum verification (IP, TCP, UDP, ICMP, etc.), IP fragment reassembly, TCP stream reassembly, protocol verification (such as insuring the IP header length is correct and the TCP data gram is not truncated), and timeout calculations. See the Gleichauf reference, column 6, lines 24-37.

The signature engine 26 of the Gleichauf reference is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signatures 30. Attack signatures 30 can comprise, for example, a rules-based hierarchy of traffic signatures of known policy violations. Signature engine 26 can compare packets from the network traffic with such attack signatures 30 such that policy violations can be discovered. See the Gleichauf reference, column 6, lines 38-45.

The Gleichauf Reference Does Not Suggest that its Firewall 16 Can be Modified

In light of the above description, it is apparent on one of ordinary skill in the art that the Gleichauf reference is focused on the network security system 20 that is external relative to the Firewall 16. The Gleichauf reference does not suggest any modifications to the operation of the Firewall 16. This becomes an important point later in this discussion because of the firewall centric publication that the Examiner proposes to combine with the Gleichauf reference.

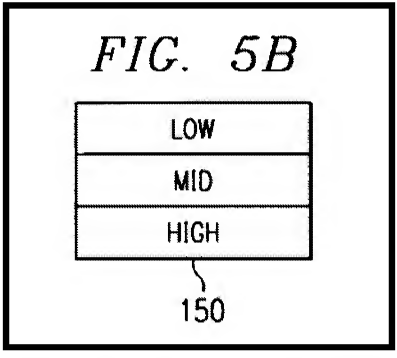
The Gleichauf Reference Does Not Use Contextual Information

Opposite to the protocol engine 24 and signature engine 26 of the Gleichauf reference, the invention described by amended independent Claim 1 monitors communications at an applications layer instead of the network and transport layers. Further, the invention as recited in amended independent Claim 1 evaluates data signatures in combination with contextual information related to data signatures. The contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature.

The Gleichauf reference evaluates protocols separately from its data signatures. That is, the Gleichauf reference uses a protocol engine 24 to evaluate protocol information separately from a signature engine 26. The Gleichauf signature engine 26 only monitors network level communications traffic for text that matches certain signatures.

Additionally, the Gleichauf reference also does not provide any teaching of a table that comprises contextual information, data signatures, and alert condition values. The Gleichauf reference also does not provide any teaching of comparing the contextual information and data signature with the table and assigning an alert condition value based on the comparison of the contextual information and data signature to data in the table.

The Examiner relies upon Figure 5B of the Gleichauf reference to address the claimed alert condition values.



The Gleichauf reference explains that Figure 5B is a prioritized attack signature list 150 that is created based upon network information gathered from a network that the security system 20 is coupled to. Gleichauf reference, column 9, lines 33-37. The Gleichauf reference explains that once it is determined that an attack signature must be disabled, as shown in FIG. 5B, low priority attack signatures can be disabled before higher priority attack signatures. Gleichauf reference, column 9, lines 55-58.

This description of Figure 5 makes it apparent to one of ordinary skill in the art that the Gleichauf reference does not provide any teaching of a creating a table comprising alert conditions values in which the alert condition values indicate a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information. The Gleichauf reference also fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

The Steinke-Firewalls Publication

The Examiner admits that the Gleichauf signature engine 26 only monitors network level communications traffic for text that matches certain signatures and that the Gleichauf reference does not use contextual information. To make up for these deficiencies, the Examiner relies upon the Steinke-Firewalls publication.

Specifically, the Examiner points the Applicant to page 2, paragraphs 1-4, of the Steinke-Firewalls publication. The last paragraph on Page 1 and Paragraphs 1-4 on page 2 of the Steinke-Firewalls publication describe an application proxy design for a firewall as follows:

> "The third firewall design is the application proxy. With a pure application proxy, no traffic at all goes through the firewall. Instead, the application proxy behaves like a server to clients on the trusted network and like a client to servers outside the trusted network.
>
> Thus, a Web browser attempting to connect to eBay will speak HTTP and pass the eBay destination URL-and the other information that browsers provide Web servers-to the application proxy firewall. The firewall will then apply its policy rules to the request. If the request is permitted, it will send the request off to eBay. The source IP address on the HTTP packets to eBay will be that of the firewall, not that of the original client.
>
> By operating at the Application layer, application proxy firewalls permit as much granularity as anyone could desire when it comes to rules. For examining, lists of specific URLs can be blocked form certain subnets, or FTP clients can be restricted from Puts, but permitted to execute Gets. Added advantages of Application-layer operation include the ability to require strong authentication before connecting and the ability to create detailed logs of security events.

> Because the action is at the Application layer, proxies must be provided for each application. A number of traditional Internet applications-including FTP, e-mail, and news are bundled into common browsers, so they can all be handled by configuring the browser to talk to the firewall. However, custom applications and network applications not bundled into a browser will have to be configured at the firewall individually, assuming they can be adapted to proxy execution at all.
>
> While application proxy firewalls can provide the highest level of security and the finest-grain control, they can also be the most complex to configure. Also, because they act as relay agents for all the clients on the network, their performance can be problematic." [Emphasis supplied.]

As noted in the last paragraph above, the Steinke-Firewalls publication explains how this proxy firewall design can be the most complex to configure and that its performance can be "problematic." The Examiner alleges that in light of the paragraphs above, it would have been obvious to combine the Steinke-Firewalls publication and the Gleichauf reference. The Applicant respectfully disagrees that one of ordinary skill in the art would combine these references for at least three reasons.

First, the statement by Steinke-Firewalls that the proxy firewall design is "problematic" would NOT motivate one of ordinary skill in the art to combine the Gleichauf reference and the Steinke-Firewalls reference. It is apparent that one of ordinary skill in the art would not combine one design with another OR add one design to another if the one design does not operate well. The Gleichauf reference explains that a technical advantage of its design is that effective intrusion detection can be had at network speeds above 50 to 60 Mps. Gleichauf reference, column 3, lines 18-20. One of ordinary skill in the art would not be motivated to add a design to the Gleichauf reference that is characterized as "problematic" when the Gleichauf reference operates at such high speeds and processes such large amounts of information.

Second, the design of the Gleichauf reference is not focused on its firewall 16, but instead on a security system 20 that is external to the firewall 16 as illustrated in Figure 2 of the Gleichauf reference. The Examiner does not explain how one of ordinary skill in the art would modify the firewall 16 of the Gleichauf reference or even the security system 20 of the Gleichauf reference. The title of the Steinke-Firewalls publication ("Firewalls") makes it clear that its design is intended only for firewalls. The lack of technical detail on what elements of the

Gleichauf reference would be modified in the Examiner's rejection makes it apparent that one of ordinary skill in the art would not combine these two references.

Third, the Applicant also notes that the Steinke-Firewalls publication may not constitute enabling prior art because of its high-level description or lack of enabling detail for its algorithms. The Applicants remind the Examiner that the Manual of Patent Examining Procedure (MPEP) requires enabling prior art to show all claimed structural features and how they interact with one another. This standard for enabling prior art is fully described in MPEP § 2121.04 (Rev. 5, August 2006), page 2100-57 that discusses how pictures may be used as prior art:

> "2121.04 Apparatus and Articles — What Constitutes Enabling Prior Art - PICTURES MAY CONSTITUTE AN 'ENABLING DISCLOSURE'
>
> Pictures and drawings may be sufficiently enabling to put the public in the possession of the article pictured. Therefore, such an enabling picture may be used to reject claims to the article. However, the picture must show all the claimed structural features and how they are put together. Jockmus v. Leviton, 28 F.2d 812 (2d Cir. 1928). See also MPEP § 2125 for a discussion of drawings as prior art."

Therefore, the Applicants respectfully submit that the Steinke-Firewalls publication cannot be used to reject any of the claims of the Applicant's invention because this publication only provides a mere naming or description of the subject matter and because it does not show "all the claimed structural features and how they are put together." Further, the Steinke-Firewalls publication even states that its "proxy firewall design can be the most complex to configure."

Even if the Examiner asserts that the Steinke-Firewalls publication is enabling prior art, the Applicants respectfully submit that this publication still does not teach every element of amended independent Claim 1 as discussed above.

The Olden Reference

The Examiner admits that the combination of the Gleichauf reference and Steinke-Firewalls publication alone do not teach the claimed combination of elements recited in each of the independent claims. Specifically, the Examiner admits that these two references do not

provide any teaching of a contextual information table. To make up for this deficiency of the Gleichauf reference and Steinke-Firewalls publication, the Examiner relies upon the Olden reference.

The Olden reference describes a security and access management system that provides for unified access management to address the specific problems facing the deployment of security for Web and non-Web environments. See Olden Abstract. The Examiner refers the Applicant to Figure 31 of the Olden reference (reproduced below) and alleges that this Figure illustrates a contextual information table as recited in Applicant's independent claims.

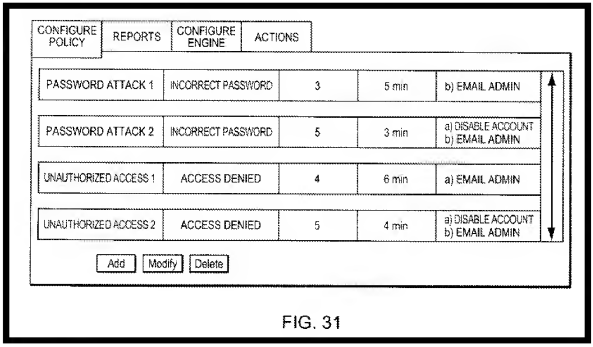


FIG. 31

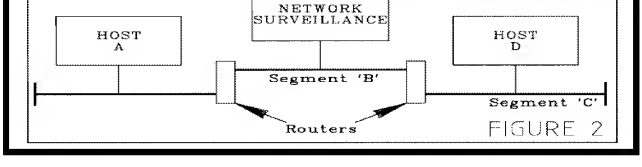
The Olden reference explains that Figure 31 is a panel that is displayed by the security and access management system to monitor attempts of unauthorized access. See Olden reference, brief description of the drawings. The Olden reference further explains that the panel of Figure 31 is for setting policies. Specifically, the policies panel maintains the list of attacks to scan for in which this list is preferably table-based, displaying the attack types. Each attack type preferably includes: Attack name, Event type, Frequency, and Action(s) to be taken. When double clicking on one of these actions, an Edit Attack dialog window will appear with the information about the attack loaded in. At the bottom of the policies panel are buttons for: Add, Modify, Delete.

One of ordinary skill in the art recognizes that the Olden reference does not provide any teaching of a contextual information table that is described by each of the amended independent claims. The Olden reference does not provide any teaching of creating a table comprising contextual information, data signatures, and alert condition values in which the contextual information comprises at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature; and the alert condition values indicate a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information. The Olden reference further fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

The Conklin Reference

The Examiner admits that the Gleichauf reference fails to teach listening for a response to a data signature from a target. To make up for this deficiency, the Examiner relies upon the Conklin reference.

The Conklin reference describes systematic monitoring, intrusion identification, notification, and tracking of unauthorized activities, such as methods or systems used by "hackers" to intrude computer networks. The Conklin reference teaches a star configuration of two Ethernet network segments 'B' and 'C' and a terminal network connection leading to a network surveillance device for a computer network as illustrated in Figure 2. The system of the Conklin reference broadcasts communications between any two computers on an Ethernet segment that is monitored by an out-of-line surveillance device. See Conklin reference, column 2, lines 58-66.



The Conklin reference explains that its intrusion detection may incorporate algorithms or patterns to detect attempted intrusions or intrusions on the network. As each packet of network data is passed from the network observation function, the intrusion detection function examines the data in comparison to a series of predefined or learned patterns which are pre-stored or developed from data received from the network.

In the Conklin reference, the network data is compared to a database of known patterns. If the collected data matches the databases stored data, individually or collectively, then the network surveillance system identifies the network data as a reportable activity and the network surveillance system components are activated and a data channel is opened between the network observation function and the evidence logging function.

Similar to the Gleichauf reference, the Conklin reference does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Conklin reference, like the Gleichauf reference, only evaluates data signatures alone without any context. The Conklin reference also does not provide any teaching of comparing contextual information and a data signature with a table and assigning an alert condition value based on the comparison of the contextual information and data signature to data in the table. The Conklin reference further fails to describe alert condition values indicating a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information. The Conklin reference also fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

The Krumel Reference

The Examiner admits that the Gleichauf reference fails to teach determining if a packet is an unknown command. To make up for this deficiency, the Examiner relies upon the Krumel reference.

The Krumel reference has a data protection system 1 that is coupled through a port to router 2 (or cable modem or other preferably broadband, persistent network connection access

device), which is linked through a broadband connection to other computer systems and networks, exemplified by Internet 8 and Internet Service Provider (ISP) 10. Packets of data are transmitted from an ISP, such as ISP 10, via Internet 8 to router 2. The packets are transmitted to data protection system 1, which analyzes the packets in "real time" and without buffering of the packets, while at the same time beginning the process of transmitting the packet to the internal network(s) in compliance with the timing requirements imposed by the Ethernet or other network standards and protocols. See Figure 1 of the Krumel reference reproduced below.

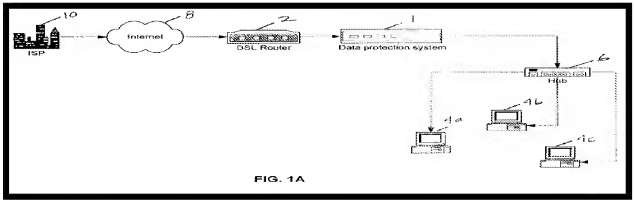


FIG. 1A

If a packet of data in the Krumel system satisfies the criteria of the rules-based filtering performed within data protection system 1, which is executed in a manner to be completed by the time the entire packet has been received by data protection system 1, then it is allowed to pass to hub 6 as a valid packet, which may then relay the cleared packet to computers 4a, 4b, 4c, etc. on the internal network. If a packet of data fails to meet the filtering criteria, then it is not allowed to pass as a valid packet and is "junked." Without the intermediate positioning of data protection system 1, the packets would be transmitted directly to unprotected hub 6, thereby exposing computers 4a, 4b and 4c to security risks. Similar filtering is performed on packets that are to be transmitted from computers 4a, 4b, and 4c to Internet 8. See the Krumel reference, page 4, paragraphs [0067-0068].

The Krumel reference explains how TCP (transmission control protocol) and UDP (user datagram protocol) packets are evaluated in parallel where TCP and UDP are host-to-host protocols located in the transport layer of the protocol stack. See Krumel reference, page 8, paragraph [0092].

Meanwhile, opposite to the Krumel reference, the invention as recited in amended independent Claim 1 evaluates data signatures at an applications layer in combination with

contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Krumel reference, like the Gleichauf reference, only evaluates data signatures alone without any context and without using a table comprising contextual information. The Krumel reference further fails to describe alert condition values indicating a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information. The Krumel reference also fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

The Zhang publication

The Examiner admits that the Gleichauf and Conklin references fail to teach suspicious behavior comprising the transmitting of a root shell prompt to a suspect node. To make up for this deficiency, the Examiner relies upon the Zhang publication.

The Zhang publication generally describes protocol specific algorithms that look for signatures particular based on different protocols. Specifically, the Zhang publication describes algorithms that find "backdoors" in a flood of legitimate network traffic. See Section 6. - Summary of the Zhang publication.

The Zhang publication does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Zhang publication, like the Gleichauf reference, only evaluates data signatures alone without any context. The Zhang publication further fails to describe alert condition values indicating a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information.

The Applicant also notes that the Zhang publication may not constitute enabling prior art because of its high-level description or lack of enabling detail for its algorithms. In light of the enablement requirements of prior art set forth by the MPEP discussed above in connection with the Steinke-Firewalls publication, the Applicants respectfully submit that the Zhang publication

cannot be used to reject any of the claims of the Applicant's invention because this publication only provides a mere naming or description of the subject matter and because it does not show "all the claimed structural features and how they are put together."

But even if the Zhang publication was enabling prior art, it still would not teach evaluating data signatures at an applications layer in combination with contextual information related to data signatures contained in a table as recited in amended independent Claim 1. This reference also fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

The Farrow publication

The Examiner admits that the Gleichauf reference fails to teach detecting a data signature of "cgi-bin/phf." To make up for this deficiency, the Examiner relies upon the Farrow publication.

The Farrow publication is a product review article that describes various intrusion detection systems that were available in July 1999. The Farrow publication mentions the "cgi-bin/phf" string in a section of the article that addresses stealth attacks. The authors of the article tested several IDS products with this string.

The Farrow publication, like the Gleichauf reference, does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Farrow publication, like the Gleichauf reference, only evaluates data signatures alone without any context and without a table comprising contextual information. The Farrow publication further fails to describe alert condition values indicating a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information.

The Applicant also notes that the Farrow publication may not constitute enabling prior art because of its high-level description of products in the market during July 1999. In light of the enablement requirements of prior art set forth by the MPEP discussed above in connection with the Steinke-Firewalls publication, the Applicants respectfully submit that the Farrow publication

cannot be used to reject any of the claims of the Applicant's invention because this publication only provides a mere naming or description of the subject matter and because it does not show "all the claimed structural features and how they are put together."

But even if the Farrow publication was enabling prior art, it still would not teach evaluating data signatures at an applications layer in combination with contextual information related to data signatures in a table as recited in amended independent Claim 1. This reference also fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

The Bernhard Reference

The Examiner admits that the Gleichauf and Conklin references fail to teach the data signature being a password in a context where filenames are likely to appear To make up for this deficiency, the Examiner relies upon the Bernhard reference.

The Bernhard reference describes a computer network 100 that includes a second line firewall 106 connected to a LAN server 112. The computer network 100 also includes a third firewall 108, a Kerberos server 110, an intranet Web server 114, a plurality of data processing systems (i.e., workstations) 116a-n, and an Internet Web server 118. All of these network elements connected to LAN 101 are monitored for computer misuse using an intrusion detection system (IDS) software 120. See Figure 1 of the Bernhard reference blow.

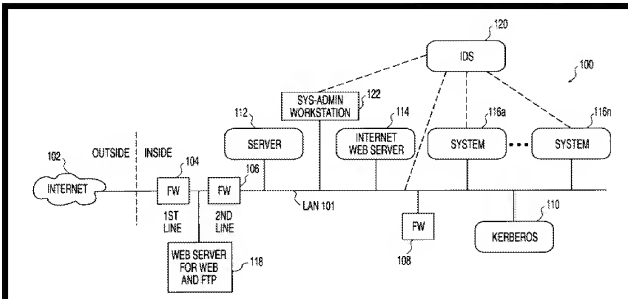


FIG. 1

The IDS software 120 of the Bernhard reference may reside and be centrally configured and monitored from a sysadmin workstation 122. The IDS software 120, as indicated in FIG. 1, may also reside on one or more of the network elements (e.g., data processing systems 116) as well as at various points within the LAN 101 between network elements (thereby acting as network-level detectors). The IDS software 120 may operate on any number of principles, such as the one specified in U.S. Pat. No. 5,557,742 issued to Smaha et al. The ARMs of the Bernhard reference operate with the particular misuse engine of the IDS software 120 selected and installed by the sysadmin of the computer network 100 in a "plug and play" manner. In other words, the ARMs reside in the IDS software 120. See the Bernhard reference, column 5, lines 1-25

The Bernhard reference explains that its product provides for automatic response to computer system misuse using active response modules (ARMs). The Bernhard reference describes steps of defining a plurality of ARMs to process instances of computer misuse, receiving an instance of misuse from an intrusion detection system (the instance of the misuse having been detected by the misuse engine) and identifying ARMs associated with and activated for the detected computer misuse. The method then, for each of the identified ARMs, collects pertinent data from the misuse engine and invokes each of the identified ARMs with the pertinent data. See the Bernhard reference, column 4, lines 26-39.

As noted above, the Bernhard reference describes what actions are taken after a security event is detected. The Bernhard reference does not relate or describe how security events are detected as evidenced above by the admission that the IDS software 120 may operate on any number of principles, such as the one specified in U.S. Pat. No. 5,557,742 issued to Smaha et al. It follows that the Bernard reference, like the Gleichauf reference, does not provide any teaching of evaluating data signatures at an applications layer in combination with contextual information related to data signatures that are contained in a table, where the contextual information can comprise at least one of an application layer data field type used to encapsulate the data signature and an application layer protocol type used to transmit the data signature. The Bernhard reference further fails to describe alert condition values indicating a security risk level relative to different data signatures and relative to other identical data signatures associated with different contextual information. This reference also fails to provide any teaching of each alert condition value comprising a ranked value that is unique to each combination of data signature and contextual information associated with a particular data signature.

Conclusion Regarding Independent Claim 1

In light of the differences between Claim 1 and the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate nor render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of this rejection of Claim 1 are respectfully requested.

THE CLAIMED INVENTION AS A WHOLE MUST BE CONSIDERED

The Applicant respectfully submits that the Examiner must evaluate the claimed combination as a whole as opposed to a defining specific isolated computer elements of the prior art which do not contemplate the specific design of the Applicants' claimed invention. The Applicants respectfully submit that M.P.E.P. section 2141.02, second paragraph (Rev. 5, August 2006), page 2100-122 states the following:

> "In determining the differences between the prior art and the claims, the question under 35 U.S.C. § 103 is not whether the differences themselves would have been obvious, but whether the

> claimed invention as a whole would have been obvious. Stratoflex, Inc. v. Aeroquip Corp., 713 F.2d 1530, 218 USPQ 871 (Fed. Cir. 1983)." [Emphasis Supplied.]

Applicant respectfully submits that the Examiner is over looking the specific design of Applicants' invention and the design presented by the prior art references. For example, the Applicant's claimed invention correlates a data signature with an application layer fingerprint of a target to determine to what extent the target is vulnerable to the data signature. This vulnerability assessment is based on the comparison that is made to the contextual information table.

Meanwhile, the Examiner has identified different computer elements of the prior art and combining them in a manner without reasonable motivation to do so. Even if the identified computer elements were combinable, they do not contemplate a vulnerability assessment as recited in the amended independent claims.

Independent Claim 14

The rejection of Claim 14 is respectfully traversed. It is respectfully submitted that the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a plurality of data signatures relevant to computer security; (2) designating an alert condition value to each data signature based on (3) each data signature itself and (4) contextual information associated with the data signature, (5) each alert condition value comprising a ranked value that (6) is unique to each combination of data signature and contextual information associated with a particular data signature, (7) the contextual information comprising at least one of (8a) an application layer data field type used to encapsulate the data signature and (8b) an application layer protocol type used to transmit the data signature, (9) the alert condition value indicating a security risk level relative to different data signatures and (10) relative to other identical data signatures associated with different contextual information; (11) creating a table comprising data signatures, contextual information, and alert condition values; (12) identifying a data signature encapsulated in an application layer data field and directed at a target using an application layer protocol; (13) evaluating a context of the data signature by one of: (14a) reviewing the application layer data field type; (14b)

reviewing the application layer protocol type; (14c) comparing the evaluated context of the data signature to the table; (15) determining whether said data signature poses a threat based on said context of said data signature; and (16) assigning an alert condition value to the data signature based on (17) the comparison of the context to data in the table, as recited in amended independent Claim 14.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of a data signature by comparing the data signature to a table comprising contextual information, as recited in amended independent Claim 14.

In light of the differences between Claim 14 and the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 14. Accordingly, reconsideration and withdrawal of this rejection of Claim 14 are respectfully requested.

Independent Claim 25

The rejection of Claim 25 is respectfully traversed. It is respectfully submitted that the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a plurality of data signatures relevant to computer security; (2) designating a relative alert condition value to each data signature based on (3) each data signature itself and (4) contextual information associated with the data signature, (5) each alert condition value comprising a ranked value that (6) is unique to each combination of data signature and contextual information associated with a particular data signature, (7) the contextual information comprising at least one of (8a) an application layer data field type used to encapsulate the data signature and (8b) an application layer protocol type used to transmit the data signature, (9) the alert condition value indicating a security risk level relative to different data signatures and (10) relative to other identical data signatures associated with different contextual information; (11) creating a table comprising contextual information, the data signatures, and the relative alert condition values; (12) monitoring a plurality of data

transmissions at an applications layer level between a suspect and a target to identify one or more data signatures, (13) said data transmissions indicating a current state of communication between said suspect and said target; (14) evaluating contextual information related to each data signature by comparing the contextual information and data signatures to the table; (15) evaluating a likelihood that said target is under attack based on (16) the contextual information of one or more data signatures of said transmissions and (17) said current state of communication; and (18) assigning a relative alert condition value to the data signature based on (19) the comparison of the contextual information to data in the table, as recited in amended independent Claim 25.

Similar to the Examiner's analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of a data signature by comparing the data signature to a table comprising contextual information, as recited in amended independent Claim 25.

In light of the differences between Claim 25 and the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 25. Accordingly, reconsideration and withdrawal of this rejection of Claim 25 are respectfully requested.

Independent Claim 37

The rejection of Claim 37 is respectfully traversed. It is respectfully submitted that the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a plurality of data signatures relevant to computer security; (2) designating a relative alert condition value to each data signature based on (3) each data signature itself and (4) contextual information associated with the data signature, (5) each alert condition value comprising a ranked value that (6) is unique to each combination of data signature and contextual information associated with a particular data signature, (7) the contextual information comprising at least one of (8a) an application layer data field type used to encapsulate the data signature and (8b) an application layer protocol type used to transmit the data signature, (9) the relative alert condition value indicating a security risk level relative to

different data signatures and (10) relative to other identical data signatures associated with different contextual information; (11) creating a table comprising contextual information, the data signatures, and the relative alert condition values; (12) detecting a data signature by evaluating communications at an application layer level between a target and a suspect; (13) correlating said data signature with a fingerprint of the target (14) to determine to what extent said target is vulnerable to said data signature; and (15) evaluating contextual information related to the data signature by (16) comparing the contextual information and the data signature to the table in order to determine a likelihood that said target is under attack; and (17) assigning a relative alert condition value to the data signature based on the (18) comparison of the contextual information and data signature to data in the table, as recited in amended independent Claim 37.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of a data signature by comparing the data signature to a table comprising contextual information, as recited in amended independent Claim 37.

In light of the differences between Claim 37 and the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 37. Accordingly, reconsideration and withdrawal of this rejection of Claim 37 are respectfully requested.

Independent Claim 50

The rejection of Claim 50 is respectfully traversed. It is respectfully submitted that the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a plurality of data signatures relevant to computer security; (2) designating an alert condition value to each data signature based on (3) each data signature itself and (4) contextual information associated with the data signature, (5) each alert condition value comprising a ranked value that (6) is unique to each combination of data signature and contextual information associated with a particular data signature, (7) the contextual information comprising at least one of (8a) an application layer data field type used to

encapsulate the data signature and (8b) an application layer protocol type used to transmit the data signature, (9) the alert condition value indicating a security risk level relative to different data signatures and (10) relative to other identical data signatures associated with different contextual information; (11) creating a table comprising data signatures, contextual information, and alert condition values; (12) identifying a data signature encapsulated in an application layer data field directed at a target using an application layer protocol; (13) evaluating a context of the data signature by one of: (14a) reviewing the application layer data field type; (14b) reviewing the application layer protocol type; and (14c) comparing the evaluated context of the data signature to the table; (15) determining whether said data signature poses a threat based on said context of said data signature; and (16) assigning an alert condition value to the data signature based on (17) the comparison of the context to data in the table, as recited in amended independent Claim 50.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of a data signature by comparing the data signature to a table comprising contextual information, as recited in amended independent Claim 50.

In light of the differences between Claim 50 and the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 50. Accordingly, reconsideration and withdrawal of this rejection of Claim 50 are respectfully requested.

Independent Claim 56

The rejection of Claim 56 is respectfully traversed. It is respectfully submitted that the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references, individually or in view of each other, fail to describe, teach, or suggest the combination of: (1) identifying a plurality of data signatures relevant to computer security; (2) designating a relative alert condition value to each data signature based on (3) each data signature itself and (4) contextual information associated with the data signature, (5) each alert condition value comprising a ranked value that (6) is unique to each combination

of data signature and contextual information associated with a particular data signature, (7) the contextual information comprising at least one of (8a) an application layer data field type used to encapsulate the data signature and (8b) an application layer protocol type used to transmit the data signature, (9) the relative alert condition value indicating a security risk level relative to different data signatures and (10) relative to other identical data signatures associated with different contextual information; (11) creating a table comprising contextual information, data signatures, and relative alert condition values; (12) monitoring a plurality of data transmissions at an applications layer level between a suspect and a target (13) to identify one or more data signatures, (14) said data transmissions indicating a current state of communication between said suspect and said target; (15) evaluating contextual information related to each data signature by (16) comparing the contextual information and data signatures to the table; (17) evaluating a likelihood that said target is under attack based on (18) the contextual information of one or more data signatures of said transmissions and (19) said current state of communication; and (20) assigning a relative alert condition value to the data signature based on (21) the comparison of the contextual information to data in the table, as recited in amended independent Claim 56.

Similar to the analysis of independent Claim 1, the Examiner's proposed combination of references fails to address the specifics of evaluating a context of a data signature by comparing the data signature to a table comprising contextual information, as recited in amended independent Claim 56.

In light of the differences between Claim 56 and the Gleichauf, Steinke-Firewalls publication, Olden, Conklin, Krumel, Zhang publication, Farrow publication, and Bernhard references mentioned above, one of ordinary skill in the art recognizes that the combination proposed by the Examiner cannot anticipate or render obvious the recitations as set forth in amended independent Claim 56. Accordingly, reconsideration and withdrawal of this rejection of Claim 56 are respectfully requested.

Dependent Claims 3-4, 6-13, 16-24, 26-36, 38-40, 42-49, 52-55, and 57

The Applicant respectfully submits that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicant also respectfully submits that the recitations of these dependent claims are of patentable significance.

In view of the foregoing, the Applicant respectfully requests that the Examiner withdraw the pending rejections of dependent Claims 3-4, 6-13, 16-24, 26-36, 38-40, 42-49, 52-55, and 57.

CONCLUSION

The foregoing is submitted as a full and complete response to the Final Office Action mailed on August 18, 2006. The Applicant and the undersigned thank Examiner Nalven for consideration of these remarks. The Applicant has amended the claims and has submitted remarks to traverse rejections of Claims 1-57. The Applicant respectfully submits that the present application is in condition for allowance. Such action is hereby courteously solicited.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any formalities that can be corrected by an Examiner's amendment, please contact the undersigned in the Atlanta Metropolitan area (404) 572-2884.

Respectfully submitted,

/SPW/
Steven P. Wigmore
Reg. No. 40,447
November 20, 2006 (MONDAY)

King & Spalding LLP
191 Peachtree Street, N.E.
Atlanta, Georgia 30303-1763
telephone: (404) 572.4600
K&S File No. 05456-105035